(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 647 981 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
28.04.2021 Bulletin 2021/17

(21) Application number: **18865893.4**

(22) Date of filing: **09.08.2018**

(51) Int Cl.:
G06F 21/56 *(2013.01)* ***G06F 21/57*** *(2013.01)*

(86) International application number:
PCT/CN2018/099570

(87) International publication number:
WO 2019/072008 (18.04.2019 Gazette 2019/16)

(54) SECURITY SCANNING METHOD AND APPARATUS FOR MINI PROGRAM, AND ELECTRONIC DEVICE

SICHERHEITSABTASTVERFAHREN UND VORRICHTUNG FÜR MINIPROGRAMM UND ELEKTRONISCHE VORRICHTUNG

PROCÉDÉ ET APPAREIL DE BALAYAGE DE SÉCURITÉ POUR UN MINI PROGRAMME ET DISPOSITIF ÉLECTRONIQUE

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **09.10.2017 CN 201710929306**

(43) Date of publication of application:
06.05.2020 Bulletin 2020/19

(73) Proprietor: **Advanced New Technologies Co., Ltd.**
George Town, Grand Cayman KY1-9008 (KY)

(72) Inventors:
- **ZHAO, Hao**
  Hangzhou
  Zhejiang 311121 (CN)
- **CAO, Shijie**
  Hangzhou
  Zhejiang 311121 (CN)
- **SHANG, Shanhu**
  Hangzhou
  Zhejiang 311121 (CN)
- **LIU, Peng**
  Hangzhou
  Zhejiang 311121 (CN)

(74) Representative: **Goddar, Heinz J.**
Boehmert & Boehmert
Anwaltspartnerschaft mbB
Pettenkoferstrasse 22
80336 München (DE)

(56) References cited:
WO-A1-2017/126786
CN-A- 103 984 697
CN-A- 106 682 561
CN-A- 106 850 209
CN-A- 107 885 995
US-A1- 2016 142 437

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 3 647 981 B1

Description

Technical Field

[0001] The present specification relates to the field of computer applications, and in particular, to a security scanning method, apparatus and electronic device for a mini program.

Background

[0002] Mini programs refer to mobile terminal APPs that are developed based on a programming language and can be used without download or installation. The most prominent characteristic of mini programs is convenient use, as the mini programs do not need to be manually installed in an operating system of a mobile terminal. However, mini programs often need to use a large APP as a carrier in use. For example, servers of some large APPs may interface with a third party's mini program development platform. After the development of a mini program is completed through a mini program development platform, a developer may release the completed mini program to the server of a large APP for interfacing with the large APP.

[0003] WO 2017/126786 A1 relates to a method for analyzing malicious code. An executable file is received and before installing the received executable file, the executable file is analyzed so as to collect suspected malicious code data from the executable file. The collected suspected malicious code data is analyzed using a probability model algorithm, so as to make a determination on the suspected malicious code data.

Summary

[0004] The invention is defined by a security scanning method for a mini program, a security scanning apparatus, and an electronic device according to the independent claims. Preferred embodiments are defined in the dependent claims.

[0005] The present specification provides a security scanning method for a mini program. the method may include:

[0006] obtaining a target mini program to be released;

[0007] invoking a security scanning strategy combination to perform multi-dimensional security scanning on the target mini program;

[0008] and when the target mini program passes the multi-dimensional security scanning, releasing the target mini program to a server corresponding to a target APP with which the target mini program is carried.

[0009] Optionally, the security scanning strategy combination comprises a combination of one or more of the following security scanning strategies:

[0010] performing malicious code scanning on the target mini program;

[0011] performing security loophole scanning on the target mini program;

[0012] and performing security loophole scanning on a server interface of the target mini program.

[0013] Optionally, the performing malicious code scanning on the target mini program comprises a combination of one or more of the scanning manners including:

[0014] detecting whether the target mini program includes a payload;

[0015] detecting whether a malicious invoking function other than authorized invoking functions defined for the target mini program exists in all the functions invoked by the target mini program;

[0016] and detecting whether media or text content invoked by the target mini program has non-compliant content.

[0017] Optionally, the performing security loophole scanning on the target mini program comprises a combination of one or more of the scanning manners including:

[0018] detecting whether the target mini program has a sensitive information leaking loophole;

[0019] detecting whether the target mini program has an HTML code loophole;

[0020] detecting whether the target mini program has a JS code loophole;

[0021] and detecting whether the target mini program has an unauthorized external resource reference loophole.

[0022] Optionally, the performing security loophole scanning on a server interface of the target mini program comprises:

[0023] parsing the server interface of the target mini program;

[0024] and performing interface loophole scanning on the parsed server interface.

[0025] The present specification further provides a security scanning apparatus for a mini program, the apparatus comprising:

[0026] an obtaining module configured to obtain a target mini program to be released;

[0027] a scanning module configured to invoke a security scanning strategy combination to perform multi-dimensional security scanning on the target mini program;

[0028] and a releasing module configured to, when the target mini program passes the multi-dimensional security scanning, release the target mini program to a server corresponding to a target APP with which the target mini program is carried.

[0029] Optionally, the scanning module further executes a combination of one or more of the following scanning strategies including:

[0030] malicious code scanning on the target mini program;

[0031] performing security loophole scanning on the target mini program;

[0032] and security loophole scanning on a server interface of the target mini program.

[0033] Optionally, the scanning module further executes a combination of one or more of the malicious code scanning manners including:

[0034] detecting whether the target mini program includes a payload;

[0035] detecting whether a malicious invoking function other than authorized invoking functions defined for the target mini program exists in all the functions invoked by the target mini program;

[0036] and detecting whether media or text content invoked by the target mini program has non-compliant content.

[0037] Optionally, the scanning module further executes a combination of one or more of the security loophole scanning manners listed below:

[0038] detecting whether the target mini program has a sensitive information leaking loophole;

[0039] detecting whether the target mini program has an HTML code loophole;

[0040] detecting whether the target mini program has a JS code loophole;

[0041] and detecting whether the target mini program has an unauthorized external resource reference loophole.

[0042] Optionally, the scanning module is further configured to:

[0043] parse the server interface of the target mini program;

[0044] and perform interface loophole scanning on the parsed server interface.

[0045] The present specification further provides an electronic device, comprising:

[0046] a processor;

[0047] and a memory configured to store executable instructions;

[0048] wherein, by executing a machine executable instruction stored in the memory and corresponding to a control logic for training a machine learning model, the processor is configured to:

[0049] obtain a target mini program to be released;

[0050] invoke a security scanning strategy combination to perform multi-dimensional security scanning on the target mini program;

[0051] and when the target mini program passes the multi-dimensional security scanning, release the target mini program to a server corresponding to a target APP with which the target mini program is carried.

[0052] In the present specification, multi-dimensional security scanning is performed on a target mini program to be released by invoking a security scanning strategy combination, and when the target mini program passes the multi-dimensional security scanning, the target mini program is then released to a server corresponding to a target APP with which the target mini program is carried, thereby effectively avoiding the release of malicious mini programs to the Internet that will impact the use security of users.

Brief Description of the Drawings

[0053]

FIG. 1 is a flow chart of a security scanning method for a mini program as illustrated in some embodiments of the present specification;

FIG. 2 is a flow chart of performing multi-dimensional security scanning on a mini program by a scanning platform as illustrated in some embodiments of the present specification;

FIG. 3 is a schematic structural diagram of hardware in an electronic device that includes a security scanning apparatus for a mini program as illustrated in some embodiments of the present specification; and

FIG. 4 is a logic block diagram of the security scanning apparatus for a mini program according to some embodiments of the present specification.

Detailed Description

[0054] The present specification provides a technical solution of performing multi-dimensional security scanning on a target mini program to be released to avoid the release of malicious mini programs to the Internet.

[0055] A server corresponding to an APP with which the target mini program is carried may interface with an independent mini program development platform. A developer may use the development platform to develop a mini program based on his/her own service needs, communicate with the server, and package and upload the developed mini program to the server for review.

[0056] The server may include a scanning platform for performing security scanning on the mini program. A security scanning strategy combination may be installed in the scanning platform in advance. When the scanning platform receives a mini program uploaded and submitted by the developer via the development platform, the scanning platform may invoke the security scanning strategy combination to perform multi-dimensional security scanning on the mini program.

[0057] In some embodiments, the security scanning strategy combination may comprise scanning strategies such as malicious code scanning on mini programs, security loophole scanning on mini programs, and security loophole scanning on a server interface of mini programs. The scanning platform may invoke the security scanning strategy combination to perform security scanning on a mini program in dimensions such as malicious code scanning, security loophole scanning, and server interface loophole scanning.

[0058] If the mini program passes the multi-dimensional security scanning, the mini program may be released to the server corresponding to the APP with which the target mini program is carried. Conversely, if the mini program does not pass the multi-dimensional security scanning, the mini program may be a malicious mini program, and the release flow of the mini program may be

directly terminated.

[0059] Therefore, the scanning platform performs multi-dimensional security scanning on a target mini program to be released by invoking a security scanning strategy combination. When the target mini program passes the multi-dimensional security scanning, the scanning platform releases the target mini program to a server corresponding to a target APP with which the target mini program is carried, thereby effectively avoiding the release of malicious mini programs to the Internet that will impact the use security of users.

[0060] The present specification will be described below with reference to exemplary embodiments and exemplary application scenarios.

[0061] FIG. 1 illustrates a security scanning method for a mini program according to some embodiments of the present specification. The method can be applied to a scanning platform to execute the following steps:

[0062] In Step 102, a target mini program to be released is obtained.

[0063] The scanning platform may, for example, comprise a service platform for performing security scanning on a target mini program to be released. In an exemplary application, the scanning platform may, for example, be deployed on a server corresponding to an APP with which the target mini program is carried. In some embodiments, when the hardware environment in which the server is installed may be a distributed server cluster, one or more physical servers may be selected from the server cluster as a hardware environment for installing the scanning platform, and the scanning platform may be constructed.

[0064] Alternatively, in another embodiment, the scanning platform may be deployed to be independent of the server. For example, the scanning platform may be independently deployed on one or more physical servers other than the server corresponding to the APP, and interface with the server corresponding to the APP.

[0065] The APP with which the target mini program is carried may, for example, comprise a native APP or a Web APP developed based on a web technology, which is not particularly defined in the present specification.

[0066] In the present specification, the server corresponding to the APP with which the target mini program is carried may further interface with an independent mini program development platform.

[0067] The mini program development platform may, for example, be a mini program development platform that is operated independently by the operator of the APP with which the target mini program is carried or a third-party mini program development platform that is in cooperation with the operator of the APP, which is not particularly defined in the present specification.

[0068] A developer may develop a mini program based on his/her own service needs through the mini program development platform. After the mini program is developed, the developer can package and upload the developed mini program to the scanning platform for security scanning. Packaging the developed mini program may refer to, for example, a process of packaging executable codes of the developed mini program to an executable program.

[0069] In some embodiments, the mini program development platform may maintain data connection with the scanning platform and provide the developer with an upload port corresponding to the developed mini program. When the mini program is developed, the developer may trigger the upload port to upload and submit the packaged mini program to the scanning platform via the data connection.

[0070] For example, the data connection may be an http connection, and the upload port may be a function button for triggering the upload of a developed mini program provided by a development platform via a visual interface.

[0071] After the developer completes the development of executable codes of the mini program, the developer may compile and package the executable codes, trigger the function button, and upload the packaged mini program to the scanning platform. When the development platform detects an event of triggering the function button at the backend, it may construct an http request packet (e.g., an http post request) at the backend for carrying the packaged mini program, then use the packaged mini program as a load carried by the http request packet, and upload the http request packet to the scanning platform via the http connection. Upon receiving the http request packet, the scanning platform may parse the http request packet and obtain the packaged mini program carried in the http request packet.

[0072] In Step 104, a security scanning strategy combination is invoked to perform multi-dimensional security scanning on the target mini program.

[0073] In the present specification, a security scanning strategy combination may be installed on the scanning platform in advance. The security scanning strategy combination may comprise pre-defined multi-dimensional security scanning strategies. Here, for a security scanning strategy in every dimension in the security scanning strategy combination, a corresponding invoking interface may be developed in advance. Upon receiving the target mini program to be released uploaded by the development platform, the scanning platform may start a security scanning flow to sequentially invoke the invoking interface of each security scanning strategy, execute each security scanning strategy, and perform multi-dimensional security scanning on the target mini program.

[0074] The invoking order of security scanning strategies in the security scanning strategy combination is not particularly defined in the present specification. A person skilled in the art may set priority for each security scanning strategy based on actual service needs, and set an invoking order for the security scanning strategies based on the priorities.

[0075] In one embodiment, the security scanning strategies in the security scanning strategy combination may, for example, comprise a combination of one or more of

the following security scanning strategies:

[0076] malicious code scanning on the target mini program;

[0077] security loophole scanning on the target mini program;

[0078] and security loophole scanning on a server interface of the target mini program.

[0079] In this case, the scanning platform may perform, by invoking the security scanning strategy combination, security scanning on the mini program in dimensions such as malicious code scanning, security loophole scanning, and server interface loophole scanning.

[0080] Taking the scanning platform performing security scanning on the target mini program to be released in three dimensions of malicious code scanning, security loophole scanning, and server interface loophole scanning as examples, detailed description will be provided below through exemplary embodiments.

[0081] FIG. 2 is a flow chart of performing multi-dimensional security scanning on the mini program by a scanning platform as illustrated in the present specification.

[0082] As shown in FIG. 2, in some embodiments, the security scanning performed by the scanning platform on the mini program may comprise three scanning dimensions of malicious code scanning, security loophole scanning, and server interface loophole scanning.

[0083] As shown in FIG. 2, in some embodiments, the malicious code scanning on the target mini program may comprise one or more scanning programs including:

[0084] a payload detection program;

[0085] a malicious function invoking detection program;

[0086] and a malicious content detection program.

[0087] The payload detection program is configured to, for example, detect whether the load of the target mini program includes a payload.

[0088] In some embodiments, a plenty of samples of known payloads may be prepared in advance, such as samples of attack codes, samples of attack data, etc. When the payload detection needs to be performed on the target mini program, all codes and data in the load of the target mini program may be parsed, and the parsed codes and data are compared with the prepared samples of known payloads and analyzed to determine whether the load of the target mini program includes a payload. If it is determined that the load of the target mini program includes a payload, the target mini program may be determined to be a malicious mini program. If the load of the target mini program does not include a payload, the target mini program may be determined to be a non-malicious mini program, and the scanning of the target mini program is passed.

[0089] The malicious function invoking detection program is configured to, for example, detect whether a malicious invoking function other than authorized invoking functions defined for the target mini program exists in all the functions invoked by the target mini program.

[0090] For example, a number of invokable authorized functions or an authorized invoking range of invokable functions may be defined in advance for each developed mini program, which may be, for example, defined by a developer in the code of the mini program or defined separately by an operator of an APP with which the target mini program is carried.

[0091] When the malicious function invoking detection needs to be performed on the target mini program, all functions invoked by the target mini program may be parsed, and whether a function other than the invokable authorized functions or a function beyond the authorized invoking range of invokable functions, exists in all the functions invoked by the target mini program may be determined. If a function other than the invokable authorized functions or a function beyond the authorized invoking range of invokable functions exists in all the functions invoked by the target mini program, a malicious function exists in all the functions invoked by the target mini program, in which case the target mini program may be determined to be a malicious mini program. Conversely, if a function other than the invokable authorized functions or a function beyond the authorized invoking range of invokable functions does not exist in all the functions invoked by the target mini program, it indicates that no malicious function exists in all the functions invoked by the target mini program, in which case the target mini program may be determined to be a non-malicious mini program, and the scanning of the target mini program is passed.

[0092] The malicious content detection program is configured to, for example, detect whether media or text content invoked by the target mini program has non-compliant content.

[0093] For example, a plenty of non-compliant content samples may be defined in advance, such as non-compliant text keywords, media fragments, and the like. When the malicious content detection needs to be performed on the target mini program, all media and text content invoked by the target mini program may be parsed, and the parsed media and text content are compared with the non-compliant content samples and analyzed to determine whether the media and text content invoked by the target mini program include non-compliant content. If it is determined that the media and text content invoked by the target mini program include non-compliant content, the target mini program may be determined to be a malicious mini program. Conversely, the target mini program may be determined to be a non-malicious mini program, and the scanning of the target mini program is passed.

[0094] As shown in FIG. 2, in some embodiments, the security loophole scanning on the target mini program may comprise one or more scanning programs including:

[0095] a sensitive information leaking loophole detection program;

[0096] an HTML code loophole detection program;

[0097] a JS code loophole detection program;

[0098] and an external resource reference loophole

detection program.

[0099] The sensitive information leaking loophole detection program is configured to, for example, detect whether the target mini program has a sensitive information leaking loophole. The HTML code loophole detection program is configured to, for example, detect whether the target mini program has an HTML code loophole. The JS code loophole detection program is configured to, for example, detect whether the target mini program has a JS code loophole. The external resource reference loophole detection program is configured to, for example, detect whether the target mini program has a security loophole that refers to an unauthorized external resource. For example, it is detected whether the target mini program refers to an unauthorized link and the like or has a loophole of unauthorized external resources other than the authorized external resources defined for the target mini program.

[0100] In some embodiments, when invoking each of the loophole scanning programs listed above to perform relevant loophole scanning on the target mini program, the scanning platform may invoke a loophole scanning tool related to each of the loophole scanning programs and installed on the scanning platform to complete the loophole scanning.

[0101] For example, the scanning platform may be installed respectively with different types of loophole scanners corresponding to a sensitive information leaking loophole, an HTML code loophole, a JS code loophole, and an external resource reference loophole, and equipped with corresponding loophole databases. Then, by running the above loophole scanners, respectively, in a software environment, the scanning platform scans the target mini program, and performs comparison with the loophole databases for analysis to identify and discover potential security loopholes in the target mini program.

[0102] When the scanning platform detects relevant security loopholes in the target mini program by executing the loophole scanning programs, the loophole scanning results may be further fed back to the developer of the target mini program to repair the relevant security loopholes. After the security loopholes are repaired, the developer may re-package and upload the target mini program via the mini program development platform for the scanning platform to perform security scanning again. When the scanning platform detects that no relevant security loopholes exist in the target mini program by executing the loophole scanning programs, the scanning of the target mini program is passed.

[0103] In addition to performing malicious code scanning and security loophole scanning on the target mini program, the scanning platform may further perform security loophole scanning on a server interface of the target mini program.

[0104] In some embodiments, the scanning platform may parse all interfaces related to the functions in the mini program, screen the parsed interfaces to obtain server interfaces of the target mini program, and then perform security loophole scanning on these server interfaces.

[0105] For example, the scanning platform may be installed with loophole scanners corresponding to server interface loopholes and equipped with corresponding loophole databases. Then, by running the above loophole scanners, respectively, in a software environment, the scanning platform scans each server interface of the target mini program, and performs comparison with the loophole databases for analysis to identify and discover potential security loopholes in these server interfaces.

[0106] When the scanning platform detects an interface loophole in a server interface of the target mini program, the loophole scanning result may be further fed back to the developer of the target mini program to repair the interface loophole. After the security loophole is repaired, the developer may re-package and upload the target mini program via the mini program development platform for the scanning platform to perform security scanning again. When no server interface loophole exists according to the scanning, the scanning of the target mini program is passed.

[0107] Here, it should be noted that it is merely an example to take the scanning platform performing security scanning on the target mini program to be released in three dimensions of malicious code scanning, security loophole scanning, and server interface loophole scanning. In some embodiments, the security scanning strategies included in the security scanning strategy combination and the dimensions of security scanning performed by the scanning platform on the target mini program may be expanded according to actual needs, which will not be enumerated in the present specification.

[0108] In Step 106, when the target mini program passes the multi-dimensional security scanning, the target mini program is released to a server corresponding to a target APP with which the target mini program is carried.

[0109] In the present specification, after the scanning platform performs multi-dimensional security scanning on the mini program by invoking the security scanning strategy combination, and if the target mini program passes the multi-dimensional security scanning, the target mini program may be determined to be a non-malicious mini program, in which case the scanning platform may start a release flow for the target mini program to further release the target mini program to the server corresponding to the APP with which the target mini program is carried and to the Internet.

[0110] If the target mini program does not pass the multi-dimensional security scanning, the target mini program may be a malicious mini program, in which case the scanning platform may block the release flow of the target mini program and terminate the release flow of the target mini program, thereby avoiding the release of malicious mini programs to the Internet that will impact the use security of users.

[0111] For example, in FIG. 2, if the target mini program passes the security scanning in dimensions such as ma-

licious code scanning, security loophole scanning, and server interface loophole scanning, respectively, the target mini program may be determined to be a non-malicious mini program and the target mini program may be normally released. Conversely, if the target mini program does not pass the security scanning in any one dimension of malicious code scanning, security loophole scanning, and server interface loophole scanning, the target mini program may be determined as a potential malicious mini program, and the scanning result may be actively fed back to the developer. After the target mini program is repaired by the developer, the multi-dimensional security scanning may be performed on the target mini program again. Alternatively, it may block the release flow of the mini program and terminate the release flow of the mini program.

[0112] The scanning platform performs multi-dimensional security scanning on a target mini program to be released by invoking a security scanning strategy combination, and when the target mini program passes the multi-dimensional security scanning, further releases the target mini program to a server corresponding to a target APP with which the target mini program is carried, thereby effectively avoiding the release of malicious mini programs to the Internet that will impact the use security of users.

[0113] Corresponding to the above method embodiments, the present specification further provides a security scanning apparatus for a mini program.

[0114] Embodiments of the security scanning apparatus for a mini program according to the present specification may be applied to an electronic device. The apparatus embodiments may be implemented by software, hardware, or a combination of software and hardware. Taking the software implementation as an example, an apparatus from the logic perspective is formed by running a corresponding computer program instruction in a non-volatile memory, by a processor of the electronic device where the apparatus is located, into an internal memory. From the hardware perspective, FIG. 3 is a schematic structural diagram of the hardware of the electronic device where the security scanning apparatus for a mini program according to the present specification is located. In addition to the processor, sensor, internal memory, network interface, and non-volatile memory shown in FIG. 3, the electronic device where the apparatus is located may further comprise other pieces of hardware according to actual functions of the electronic device, which will not be elaborated herein.

[0115] FIG. 4 is a block diagram of the security scanning apparatus for a mini program according to some embodiments of the present specification.

[0116] Referring to FIG. 4, the security scanning apparatus 40 for a mini program may be applied to the electronic device shown in FIG. 3, the apparatus comprising: an obtaining module 401, a scanning module 402, and a releasing module 403.

[0117] The obtaining module 401 is configured to obtain a target mini program to be released.

[0118] The scanning module 402 is configured to invoke a security scanning strategy combination to perform multi-dimensional security scanning on the target mini program.

[0119] The releasing module 403 is configured to, when the target mini program passes the multi-dimensional security scanning, release the target mini program to a server corresponding to a target APP with which the target mini program is carried.

[0120] In some embodiments, the scanning module 402 is further configured to execute one or more of:

[0121] malicious code scanning on the target mini program;

[0122] security loophole scanning on the target mini program;

[0123] and security loophole scanning on a server interface of the target mini program.

[0124] In some embodiments, the scanning module 402 further executes a combination of one or more of the malicious code scanning manners listed below:

[0125] detecting whether the target mini program includes a payload;

[0126] detecting whether a malicious invoking function other than authorized invoking functions defined for the target mini program exists in all the functions invoked by the target mini program;

[0127] and detecting whether media or text content invoked by the target mini program has non-compliant content.

[0128] In some embodiments, the scanning module 402 is further configured to execute one or more security loophole scanning operations including:

[0129] detecting whether the target mini program has a sensitive information leaking loophole;

[0130] detecting whether the target mini program has an HTML code loophole;

[0131] detecting whether the target mini program has a JS code loophole;

[0132] and detecting whether the target mini program has an unauthorized external resource reference loophole.

[0133] In some embodiments, the scanning module 402 is further configured to:

[0134] parse the server interface of the target mini program;

[0135] and perform interface loophole scanning on the parsed server interface.

[0136] Since the apparatus embodiment substantially corresponds to the method embodiment, the description of the method embodiment may be referenced. The above-described apparatus embodiment is merely exemplary, wherein the units described as discrete parts may or may not be physically separated. The parts shown as units may or may not be physical units, i.e., the parts may be located at the same place or may be distributed over a plurality of network units. Some or all of the modules thereof may be selected according to actual needs

to achieve the objective of the solutions of the present specification. Those of ordinary skills in the art may understand and implement the apparatus embodiment without inventive effort.

[0137] The system, apparatus, module or unit described in the above embodiments may be, for example, implemented by a computer chip or entity, or implemented by a product having the functions. A typical implementation device is a computer. In one example, a computer may be, for example, a server, a personal computer, a laptop computer, a cellular phone, a camera phone, a smart phone, a personal digital assistant, a medium player, a navigation device, an email receiving and transmitting device, a game console, a tablet computer, a wearable device, or a combination of any devices in these devices.

[0138] Corresponding to the above method embodiments, the present specification further provides an electronic device comprising: a processor and a memory configured to store machine executable instructions, wherein the processor and the memory may be connected to each other via an internal bus. In some embodiments, the device may further comprise an external interface for communications with other devices or parts.

[0139] In some embodiments, by executing the executable instruction stored in the memory and corresponding to a control logic of security scanning for a mini program, the processor is configured to

[0140] obtain a target mini program to be released;

[0141] invoke a security scanning strategy combination to perform multi-dimensional security scanning on the target mini program;

[0142] and when the target mini program passes the multi-dimensional security scanning, release the target mini program to a server corresponding to a target APP with which the target mini program is carried.

[0143] In some embodiments, by executing the executable instruction stored in the memory and corresponding to a control logic of security scanning for a mini program, the processor is further configured to execute one or more operations including:

[0144] performing malicious code scanning on the target mini program;

[0145] performing security loophole scanning on the target mini program;

[0146] and performing security loophole scanning on a server interface of the target mini program.

[0147] In some embodiments, by executing the executable instruction stored in the memory and corresponding to a control logic of security scanning for a mini program, the processor is further configured to execute one or more operations including:

[0148] detecting whether the target mini program includes a payload;

[0149] detecting whether a malicious invoking function other than authorized invoking functions defined for the target mini program exists in all the functions invoked by the target mini program;

[0150] and detecting whether media or text content invoked by the target mini program has non-compliant content.

[0151] In some embodiments, by executing the executable instruction stored in the memory and corresponding to a control logic of security scanning for a mini program, the processor is further configured to execute one or more operations including:

[0152] detecting whether the target mini program has a sensitive information leaking loophole;

[0153] detecting whether the target mini program has an HTML code loophole;

[0154] detecting whether the target mini program has a JS code loophole;

[0155] and detecting whether the target mini program has an unauthorized external resource reference loophole.

[0156] In some embodiments, by executing the executable instruction stored in the memory and corresponding to a control logic of security scanning for a mini program, the processor is further configured to

[0157] parse the server interface of the target mini program;

[0158] and perform interface loophole scanning on the parsed server interface.

[0159] It would be easy for those of ordinary skills in the art to, after considering the present specification and practicing the invention disclosed herein, conceive of other implementation manners of the present specification. The present specification is intended to encompass any variations, uses or adaptive changes of the present specification, and these variations, uses or adaptive changes follow general principles of the present specification and comprise common general knowledge or common technical means in the art that are not disclosed in the present specification. The present specification and embodiments are regarded to be merely exemplary, and the true scope and spirit of the present specification shall be subject to the appended claims.

[0160] It should be understood that the present specification is not limited to the accurate structure described above and illustrated in the accompanying drawings, and various modifications and changes may be made to the present specification without departing from the scope thereof. The scope of the present specification shall be only subject to the appended claims.

[0161] Particular embodiments of the present specification are described above, and other embodiments fall within the scope of the appended claims. In some cases, actions or steps stated in the claims may be executed in an order different from those in the embodiments and can still achieve desired results. In addition, a process depicted in the accompanying drawings does not necessarily require the illustrated particular order or continuous order to achieve desired results. In some implementation manners, multi-task processing and parallel processing may be feasible or may be beneficial.

[0162] The above description are merely preferred em-

bodiments of the present specification, which are not used to limit the present specification.

Claims

1. A security scanning method for a mini program, the method comprising:

   obtaining (102) a target mini program to be released;
   invoking (104) a security scanning strategy combination to perform multi-dimensional security scanning on the target mini program, wherein the security scanning strategy combination comprises malicious code scanning on the target mini program, security loophole scanning on the target mini program, and
   security loophole scanning on a server interface of the target mini program, and
   wherein the security loophole scanning on the target mini program comprises:

      detecting whether the target mini program includes a sensitive information leaking loophole;
      detecting whether the target mini program includes an HTML code loophole;
      detecting whether the target mini program includes a JS code loophole; and
      detecting whether the target mini program includes an unauthorized external resource reference loophole; and

   when (106) the target mini program passes the multi-dimensional security scanning,
   releasing the target mini program to a server corresponding to a target APP which the target mini program uses as a carrier in use.

2. The method according to claim 1, wherein the malicious code scanning on the target mini program comprises one or more of:

   detecting whether the target mini program includes a payload;
   detecting whether a malicious invoking function, other than an authorized invoking function defined for the target mini program, is present in functions invoked by the target mini program; and
   detecting whether media or text content invoked by the target mini program includes non-compliant content.

3. The method according to claim 1 or 2, wherein the security loophole scanning on a server interface of the target mini program comprises:

   parsing the server interface of the target mini program; and
   performing interface loophole scanning on the parsed server interface.

4. A security scanning apparatus for a mini program, the apparatus comprising:

   an obtaining module (401) configured to obtain a target mini program to be released;
   a scanning module (402) configured to invoke a security scanning strategy combination to perform multi-dimensional security scanning on the target mini program, wherein the security scanning strategy combination comprises malicious code scanning on the target mini program, security loophole scanning on the target mini program, and security loophole scanning on a server interface of the target mini program, and wherein the security loophole scanning on the target mini program comprises, and wherein the scanning module (402) is further configured to execute the security loophole scanning by:

      detecting whether the target mini program includes a sensitive information leaking loophole;
      detecting whether the target mini program includes an HTML code loophole;
      detecting whether the target mini program includes a JS code loophole; and
      detecting whether the target mini program includes an unauthorized external resource reference loophole; and

   a releasing module (403) configured to, when the target mini program passes the multi-dimensional security scanning, release the target mini program to a server corresponding to a target APP which the target mini program uses as a carrier in use.

5. The apparatus according to claim 4, wherein the scanning module (402) is configured to execute one or more of malicious code scanning programs including:

   detecting whether the target mini program includes a payload;
   detecting whether a malicious invoking function, other than authorized invoking functions defined for the target mini program, is present in functions invoked by the target mini program; and
   detecting whether media or text content invoked by the target mini program includes non-compliant content.

6. The apparatus according to claim 4 or 5, wherein the

scanning module is further configured to:

parse the server interface of the target mini program; and
perform interface loophole scanning on the parsed server interface.

Patentansprüche

1. Sicherheitsscanverfahren für ein Miniprogramm, wobei das Verfahren Folgendes umfasst:

Erhalten (102) eines Zielminiprogramms, das zu veröffentlichen ist;
Aufrufen (104) einer Sicherheitsscanstrategiekombination zum Durchführen eines mehrdimensionalen Sicherheitsscans am Zielminiprogramm, wobei die Sicherheitsscanstrategiekombination das Scannen nach Schadcode am Zielminiprogramm, das Scannen nach einer Sicherheitslücke am Zielminiprogramm und das Scannen nach einer Sicherheitslücke an einer Serverschnittstelle des Zielminiprogramms umfasst und wobei das Scannen nach einer Sicherheitslücke am Zielminiprogramm Folgendes umfasst:

Detektieren, ob das Zielminiprogramm eine Lücke für den Zugang zu empfindlichen Informationen beinhaltet;
Detektieren, ob das Zielminiprogramm eine Lücke für HTML-Code beinhaltet;
Detektieren, ob das Zielminiprogramm eine Lücke für JS-Code beinhaltet; und
Detektieren, ob das Zielminiprogramm eine Lücke für einen Verweis auf eine unbefugte externe Ressource beinhaltet; und
wenn (106) das Zielminiprogramm den mehrdimensionalen Sicherheitsscan besteht, Veröffentlichen des Zielminiprogramms für einen Server, der einer Ziel-APP entspricht, die das Zielminiprogramm bei Verwendung als einen Träger verwendet.

2. Verfahren nach Anspruch 1, wobei das Scannen auf Schadcode am Zielminiprogramm eines oder mehreres von Folgendem umfasst:

Detektieren, ob das Zielminiprogramm Nutzdaten beinhaltet;
Detektieren, ob, abgesehen von einer autorisierten Aufruffunktion, die für das Zielminiprogramm definiert ist, eine bösartige Aufruffunktion in Funktionen, die vom Zielminiprogramm aufgerufen werden, vorhanden ist; und
Detektieren, ob ein Medien- oder Textinhalt, der vom Zielminiprogramm aufgerufen wird, einen nicht konformen Inhalt beinhaltet.

3. Verfahren nach Anspruch 1 oder 2, wobei das Scannen nach einer Sicherheitslücke an einer Serverschnittstelle des Zielminiprogramms Folgendes umfasst:

Parsen der Serverschnittstelle des Zielminiprogramms und
Durchführen eines Scans auf eine Schnittstellenlücke an der geparsten Serverschnittstelle.

4. Sicherheitsscanvorrichtung für ein Miniprogramm, wobei die Vorrichtung Folgendes umfasst:

ein Erhaltungsmodul (401), das dazu ausgelegt ist, ein Zielminiprogramm, das zu veröffentlichen ist, zu erhalten;
ein Scanmodul (402), das dazu ausgelegt ist, eine Sicherheitsscanstrategiekombination zum Durchführen eines mehrdimensionalen Sicherheitsscans am Zielminiprogramm aufzurufen, wobei die Sicherheitsscanstrategiekombination das Scannen nach Schadcode am Zielminiprogramm, das Scannen nach einer Sicherheitslücke am Zielminiprogramm und das Scannen nach einer Sicherheitslücke an einer Serverschnittstelle des Zielminiprogramms umfasst und wobei das Scannen nach einer Sicherheitslücke am Zielminiprogramm Folgendes umfasst und wobei das Scanmodul (402) ferner dazu ausgelegt ist, das Scannen auf eine Sicherheitslücke durch Folgendes auszuführen:

Detektieren, ob das Zielminiprogramm eine Lücke für den Zugang zu empfindlichen Informationen beinhaltet;
Detektieren, ob das Zielminiprogramm eine Lücke für HTML-Code beinhaltet;
Detektieren, ob das Zielminiprogramm eine Lücke für JS-Code beinhaltet; und
Detektieren, ob das Zielminiprogramm eine Lücke für einen Verweis auf eine unbefugte externe Ressource beinhaltet; und
ein Veröffentlichungsmodul (403), das dazu ausgelegt ist,
wenn das Zielminiprogramm den mehrdimensionalen Sicherheitsscan besteht, das Zielminiprogramm für einen Server zu veröffentlichen, der einer Ziel-APP entspricht, die das Zielminiprogramm bei Verwendung als einen Träger verwendet.

5. Vorrichtung nach Anspruch 4, wobei das Scanmodul (402) dazu ausgelegt ist, ein oder mehrere Scanprogramme für Schadcode auszuführen, die Folgendes beinhalten:

Detektieren, ob das Zielminiprogramm Nutzdaten beinhaltet;
Detektieren, ob, abgesehen von autorisierten Aufruffunktionen, die für das Zielminiprogramm definiert sind, eine bösartige Aufruffunktion in Funktionen, die vom Zielminiprogramm aufgerufen werden, vorhanden ist; und
Detektieren, ob ein Medien- oder Textinhalt, der vom Zielminiprogramm aufgerufen wird, einen nicht konformen Inhalt beinhaltet.

6. Vorrichtung nach Anspruch 4 oder 5, wobei das Scanmodul ferner zu Folgendem ausgelegt ist:

Parsen der Serverschnittstelle des Zielminiprogramms und
Durchführen eines Scans auf eine Schnittstellenlücke an der geparsten Serverschnittstelle.

Revendications

1. Procédé d'analyse de sécurité pour un mini-programme, le procédé comprenant de :

obtenir (102) un mini-programme cible à publier;
appeler (104) une combinaison de stratégies d'analyse de sécurité pour effectuer une analyse de sécurité multidimensionnelle sur le mini-programme cible, dans lequel la combinaison de stratégies d'analyse de sécurité comprend l'analyse de code malveillant sur le mini-programme cible, l'analyse des failles de sécurité sur le mini-programme cible, et l'analyse des failles de sécurité sur une interface serveur du mini-programme cible, et dans lequel l'analyse des failles de sécurité sur le mini-programme cible comprend de :

détecter si le mini-programme cible comprend une faille de fuite d'informations sensibles;
détecter si le mini-programme cible comprend une faille de code HTML;
détecter si le mini-programme cible comprend une faille de code JS; et
détecter si le mini-programme cible comprend une faille de référence de ressource externe non autorisée; et
lorsque (106) le mini-programme cible réussit l'analyse de sécurité multidimensionnelle, publier le mini-programme cible sur un serveur correspondant à une application cible que le mini-programme cible utilise comme support en cours d'utilisation.

2. Procédé selon la revendication 1, dans lequel l'analyse de code malveillant sur le mini-programme cible comprend l'un ou plusieurs parmi de :

détecter si le mini-programme cible comprend une charge utile;
détecter si une fonction d'appel malveillante, autre qu'une fonction d'appel autorisée définie pour le mini-programme cible, est présente dans des fonctions appelées par le mini-programme cible; et
détecter si un contenu multimédia ou textuel appelé par le mini-programme cible comprend un contenu non conforme.

3. Procédé selon la revendication 1 ou 2, dans lequel l'analyse des failles de sécurité sur une interface serveur du mini-programme cible comprend de :
analyser l'interface serveur du mini-programme cible; et effectuer une analyse des failles d'interface sur l'interface serveur analysée.

4. Appareil d'analyse de sécurité pour un mini-programme, l'appareil comprenant :

un module d'obtention (401) configuré pour obtenir un mini-programme cible à publier;
un module d'analyse (402) configuré pour appeler une combinaison de stratégies d'analyse de sécurité pour effectuer une analyse de sécurité multidimensionnelle sur le mini-programme cible, dans lequel la combinaison de stratégies d'analyse de sécurité comprend l'analyse de code malveillant sur le mini-programme cible, l'analyse des failles de sécurité sur le mini-programme cible, et
l'analyse des failles de sécurité sur une interface serveur du mini-programme cible, et dans lequel l'analyse des failles de sécurité sur le mini-programme cible comprend de, et dans lequel le module d'analyse (402) est en outre configuré pour exécuter l'analyse des failles de sécurité en :

détectant si le mini-programme cible comprend une faille de fuite d'informations sensibles;
détectant si le mini-programme cible comprend une faille de code HTML;
détectant si le mini-programme cible comprend une faille de code JS; et
détectant si le mini-programme cible comprend une faille de référence de ressource externe non autorisée; et
un module de publication (403) configuré pour, lorsque le mini-programme cible réussit l'analyse de sécurité multidimensionnelle, publier le mini-programme cible sur un serveur correspondant à une application cible que le mini-programme cible utilise com-

me support en cours d'utilisation.

5. Appareil selon la revendication 4, dans lequel le module d'analyse (402) est configuré pour exécuter un ou plusieurs programmes d'analyse de code malveillant comprenant de :

détecter si le mini-programme cible comprend une charge utile;
détecter si une fonction d'appel malveillante, autre que des fonctions d'appel autorisées définies pour le mini-programme cible, est présente dans des fonctions appelées par le mini-programme cible; et
détecter si un contenu multimédia ou textuel appelé par le mini-programme cible comprend un contenu non conforme.

6. Appareil selon la revendication 4 ou 5, dans lequel le module d'analyse est en outre configuré pour : analyser l'interface serveur du mini-programme cible; et effectuer une analyse des failles d'interface sur l'interface serveur analysée.

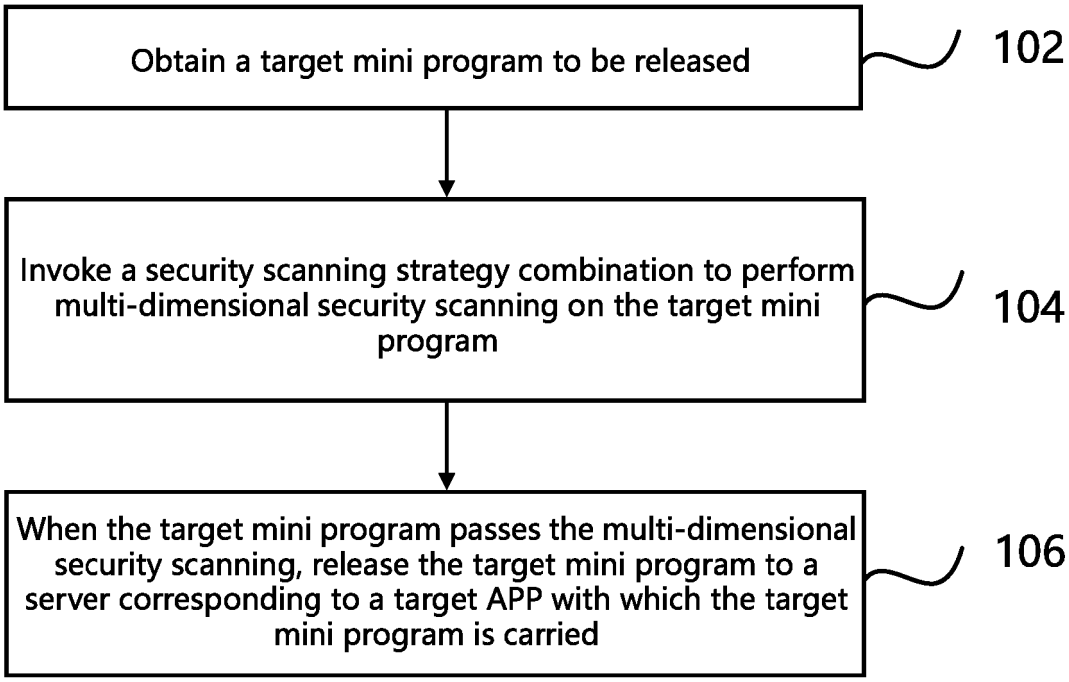
Obtain a target mini program to be released
102
Invoke a security scanning strategy combination to perform multi-dimensional security scanning on the target mini program
104
When the target mini program passes the multi-dimensional security scanning, release the target mini program to a server corresponding to a target APP with which the target mini program is carried
106

FIG. 1

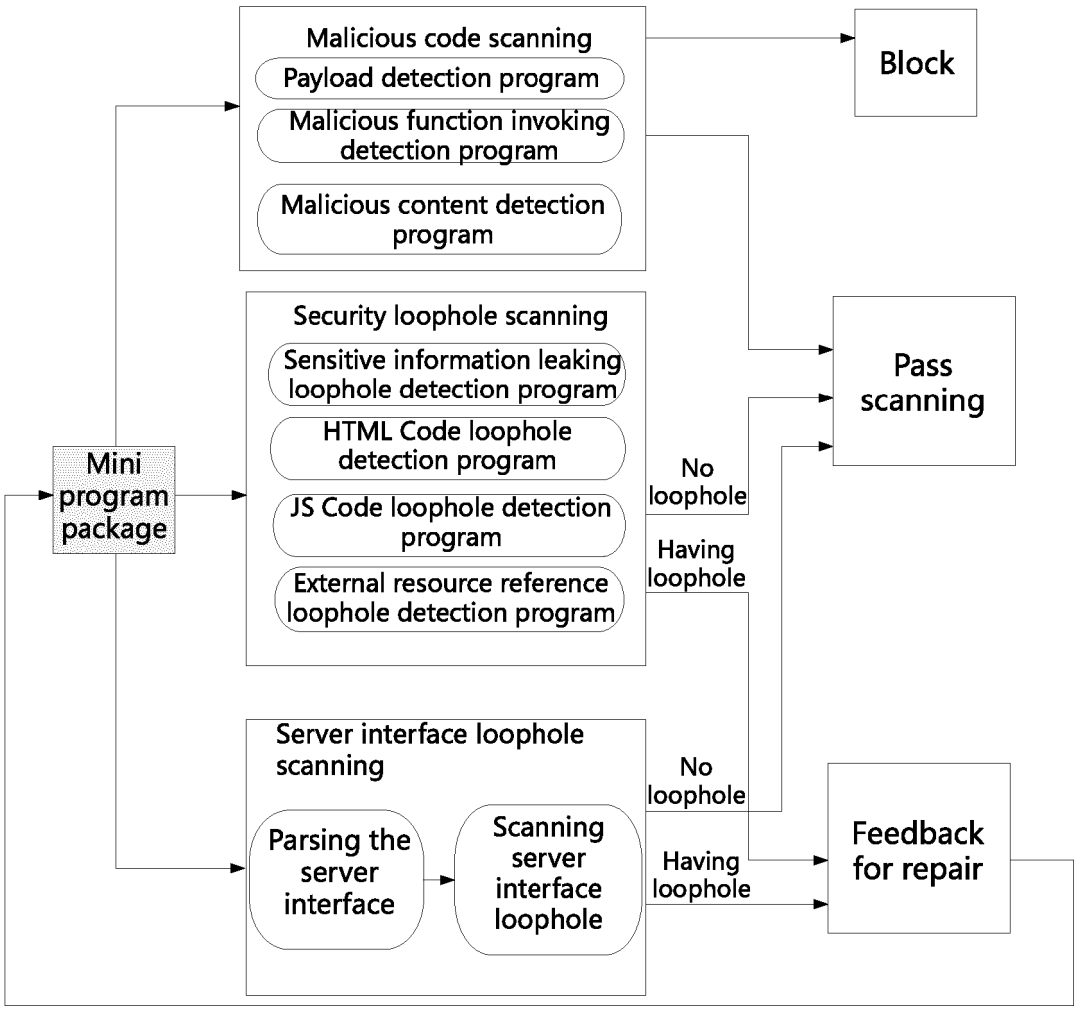
Malicious code scanning
Payload detection program
Malicious function invoking detection program
Malicious content detection program
Block
Security loophole scanning
Sensitive information leaking loophole detection program
HTML Code loophole detection program
JS Code loophole detection program
External resource reference loophole detection program
Pass scanning
Mini program package
No loophole
Having loophole
Server interface loophole scanning
Parsing the server interface
Scanning server interface loophole
No loophole
Having loophole
Feedback for repair
Developer re-packages after repairing the loophole

FIG. 2

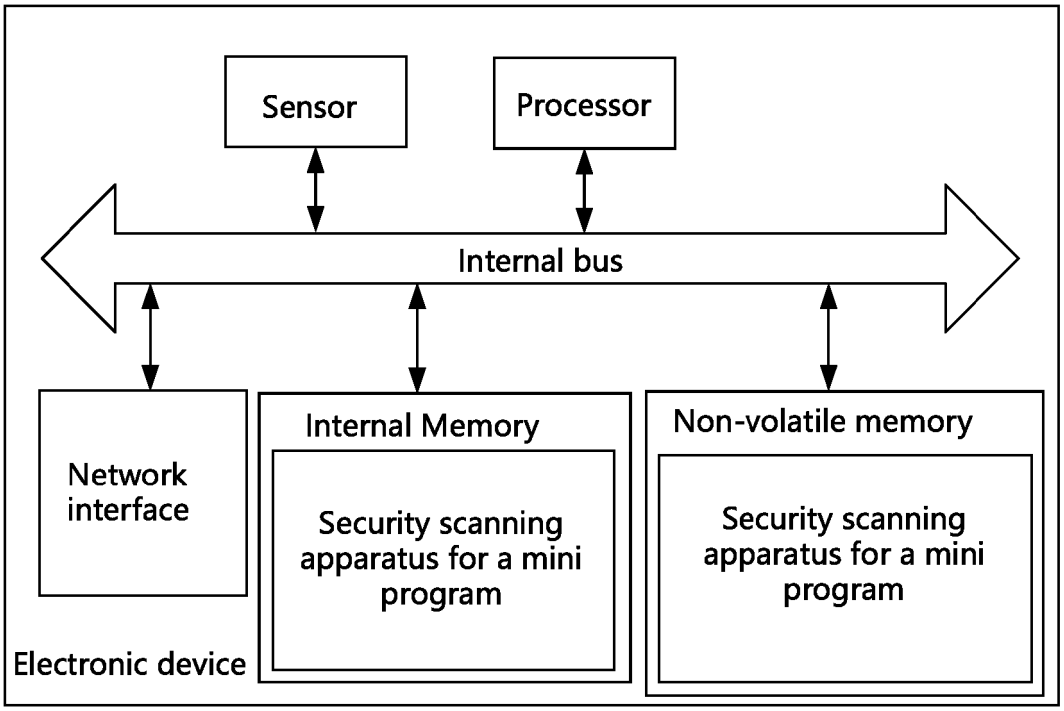
Sensor
Processor
Internal bus
Network interface
Internal Memory
Security scanning apparatus for a mini program
Non-volatile memory
Security scanning apparatus for a mini program
Electronic device

FIG. 3

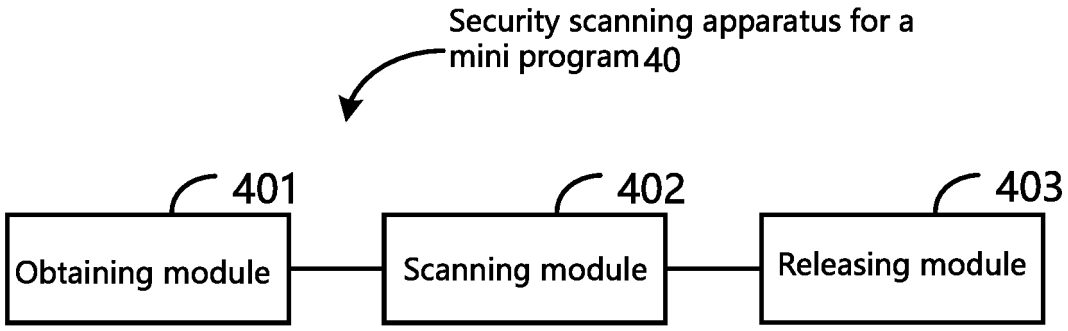
Security scanning apparatus for a mini program 40
401
Obtaining module
402
Scanning module
403
Releasing module

FIG. 4

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- WO 2017126786 A1 **[0003]**